UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,398	02/17/2004	Valiuddin Ali	200314072-1	1614

22879 7590 12/11/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	**PAPER NUMBER**
2437	

NOTIFICATION DATE	DELIVERY MODE
12/11/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/780,398
Filing Date: February 17, 2004
Appellant(s): ALI ET AL.

Anthony F. Bonner, Jr.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/12/09 appealing from the Office action mailed 8/12/08.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

EP1111495A1	**Thompson et al.**	**6-2001**

(Thompson)

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 14 – 18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Specifically, these claims broadly recite computer elements as software per se (see par. 12, 13, 16 and fig. 1:70, 80 of applicant's specification).

[0012] In the embodiment illustrated in FIG. 1, client 12 also comprises a security module 70 for controlling access by client 12 to various types of secure or protected computer resources. … Security module 70 may comprise software, hardware, or a combination of software and hardware. …

[0013] As illustrated in FIG. 1, security module 70 comprises a collection module 80, a recovery module 82, and an

encryption/decryption module 84. Briefly, collection module 80 is used to acquire various types of information from a user of client 12 to enable the user of client 12 to recover a password or other type of security credential for accessing or initiating operations associated with a secure computer resource independent of a computer resource external to client 12. …

[0016] In some embodiments, for a secure client 12 booting or initialization application, BIOS 62 is configured to automatically initiate or activate collection module 80 during an initial client 12 access by a particular user to acquire or otherwise determine verification data 94 associated with the user. … Verification data 94 may also be acquired or otherwise determined at a variety of levels (e.g., provided to BIOS 62 through any operating system layer software driver or application).

…

Herein, the applicant explicitly discloses the recited means (i.e. security module, comprising collection module 80) to be software per se. [e.g. “software”, and/or a “software driver”, “application”].

The examiner notes that claims comprising means of which are broadly and reasonably interpreted to be limited to software instructions per se. fail to fall within any one of the statutory categories of invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1 – 46 are rejected under 35 U.S.C. 102(b) as being anticipated by Thompson et al. (Thompson), "Device Security Mechanism Based on Registered Passwords", EP 1,111,495 A1.

Regarding claim 1, Thompson discloses:

a processor; and a memory component that stores (fig. 2:100)*:*

a security module (fig. 2:108) *adapted to control access to a secure computer resource by a user via a client* (fig. 2:100) *based on verification of a security credential provided by the user* (fig. 2:108; par. 11, 12);

and verification data disposed on the client and accessible by the security module (fig. 4:404, 406, 408, 412, 414, 416, 418). Herein disclosed is information disposed on the client which implements a recovery mechanism [i.e. "verification data"] to enable the user of client 12 to independently recover a security credential.

the security module adapted to enable the user to recover the security credential from the client based on a response received from the user associated with the verification data (fig. 6; par. 23). Herein, Thompson discloses that the user, via the query/response mechanism, is able to "recover" his/her password (i.e. "security

credential) after the security module receives a "response from the user" (i.e. password), compares the received password with the stored password belonging to the user (fig. 6:606), and allows the user to reset/modify his or her password (fig. 6: 610, 612).

For the purpose of examination, the examiner interprets *"to recover the security credential from the client"* in a manner consistent with the applicant's specification. Specifically, the applicant states in paragraph 15, *"For example, as used herein, "recovering" security credential 100 includes enabling the user to independently retrieve security credential 100,* ***enabling the user to independently reset security credential*** *100, and/or automatically having security credential 100 reset for the user by security module 70 without assistance from support personnel or an external computer resource*." Thus, as Thompson discloses that the security module enables to user to independently reset the security credential (i.e. password), the examiner notes that Thompson discloses enabling the user to "recover" the security credential.

It is furthermore noted, that Thompson discloses that, via the query/response mechanism, the security module receives a "response from the user" (i.e. password), compares the received password with the stored password belonging to the user (fig. 6:606), and then based upon a valid "response", allows the password to be reset and stored such that the user is enabled to retrieve it at any time in case he/she should forget it (fig. 6:606, 610; 616; col. 9: lines 18-21). Thus, Thompson discloses that the user is enabled to retrieve his password, which consistent with the applicant's specification, may be interpreted as a form of "recovering".

Regarding claim 2, Thompson discloses:

wherein the security module is adapted to enable the user to reset the security credential based on the response (fig. 6:610; see also fig. 4:414).

Regarding claim 3, Thompson discloses:

wherein the security module is adapted to generate a query to present to the user based on the verification data (fig. 6:602,608,610).

Regarding claim 4, Thompson discloses:

wherein the security module is adapted to control booting of the client based on the response (Abstract).

Regarding claim 5, Thompson discloses:

wherein the security module is adapted to initiate a collection module to acquire the verification data from the user (fig. 4).

Regarding claim 6, Thompson discloses:

wherein the security module is adapted to encrypt the security credential based on the verification data (fig. 4:406).

Regarding claim 7, Thompson discloses:

wherein the security module is adapted to decrypt an encrypted security credential based on the response (par. 22).

Regarding claim 8, Thompson discloses:

wherein the security module is disposed in a basic input/output system (BIOS) (par. 11).

Regarding claim 9, Thompson discloses:

wherein the security module is adapted to control access to a secure communications network (col. 6:40-44 – access to the operations of the client [i.e. network access], is controlled).

Regarding claim 10, Thompson discloses:

wherein the security module is adapted to control access to a computer network resource (col. 6:40-44 – access to the operations of the client [i.e. network resource access] is controlled).

Regarding claim 11, Thompson discloses:

wherein the security module is adapted to enable the user to retrieve the security credential based on the response (fig. 6:606, 610; 616; col. 9: lines 18-21).

Regarding claim 12, Thompson discloses:

wherein the security module is adapted to automatically reset the security credential based on the response (fig. 6:610,612,614,616,618).

Regarding claim 13, Thompson discloses:

wherein the security module is disposed on the client (fig. 2).

Regarding claims 14 – 46, they are system method and means claims essentially corresponding to claims 1 – 13, and they are rejected, at least, for the same reasons.

(10) Response to Argument

Appellant argues or asserts essentially that:

First, the present application clearly discloses structure for each of the claim elements of claims 14- 18. More specifically, the as illustrated on page 3, among other places, the present application discloses a "client 12 [that] comprises a processor or central processing unit (CPU) 20; a memory 22 having an operating system 24..." (paragraph [0010]). Further, on page 8, the present application discloses that the "[s]ecurity module 70 may comprise software, hardware, or a combination of software and hardware" (paragraph [0012]).

As illustrated in the above cited passages of the written description, at least one embodiment for a "means for controlling" and a means for accessing" of claim 14, for example, includes a specific hardware component (e.g., a processor and/or memory

component) that is configured to implement the claimed function. Similarly, other embodiments may include a processor and/or a memory (and/or other components) that facilitate the recited function. (Brief, pg. 6, par. 2, 3)

Examiner respectfully responds:

In response, the examiner respectfully notes that the appellant is mistaken, as the appellant's specification explicitly teaches that the multitude of device, noted by the applicant (e.g. see Specification, par. 10 – i.e. CPU 20, memory 22, input devices 28, output devices 30, storage controller 40, network interface 50, etc.) are comprised within the *client 12*, **not** the claimed *security module 70*, comprising *collection module 80*.

Regarding the latter mentioned *security module 70*, comprising *collection module 80*, the appellant has clearly and explicitly identified them to be the recited means (e.g. see Specification, par. 12, 13), wherein these recited means are said to comprise software per se. (e.g. see Specification, par. 12, *"Security module 70 may comprise software, hardware, or a combination of software and hardware"*) . Furthermore, appellant has admitted on record that these "modules" are the means recited within the claims [e.g. see Brief, pg. 3, *"…means for controlling access (page 3, line 26 and FIG. 1, element 70 "a security module 70 for controlling access...") … and means for accessing verification data (page 5, line 22 and FIG. 1, element 80 "activate collection*

module 80 during an initial client 12 access by a particular user to acquire or otherwise determine verification data 94")…"].

Thus, the examiner notes that the claims reciting only means of which are broadly and reasonably interpreted to be limited to software instructions per se. fail to fall within any one of the statutory categories of invention.

Appellant argues or asserts essentially that:

Second, the Examiner's statement is technologically incorrect. More specifically, as indicated above, the Examiner argues "[A]pplicant has shown within the [A]pplicant's specification that the recited means of claims 14 - 18 are implemented as software." This is an incorrect statement. As is clearly evident to one of ordinary skill in the art, software is merely a set of instructions that may be executed by computer hardware to perform one or more actions. Accordingly, software cannot perform any function of claims 14 - 18 without interaction with hardware. As a nonlimiting example, software (acting exclusively) cannot "access a secure computer resource" (claim 14) without being executed on computer hardware. Consequently, the "means for' terminology that precedes the recited function must include hardware. (Brief, pg. 7, par. 1)

Examiner respectfully responds:

In response, the examiner respectfully notes that the appellant is mistaken. Specifically, the appellant's remarks do not prove that the recited software means (i.e. *security module 70*, comprising *collection module* 80) must also comprise hardware.

Instead, the appellant's argument merely emphasizes the limitations of software alone. Essentially, software means would be rendered ineffective or useless without some form of hardware means. Yet, this well known fact does not in any way suggest that recitations of software are inherently the same as recitations of hardware. Rather, this fact supports the reasons given by the examiner for the rejection of these claims under 35 U.S.C. 101 for claiming non-statutory subject matter. Claims 14 -18 fail to comprise recitations of hardware and are thus noted as not falling within the scope of any statutory category of invention (i.e. "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof").

Appellant argues or asserts essentially that:

The Examiner referred to the specification to determine the proper scope of claim elements, but improperly analyzes the passage cited from the specification. More specifically, beginning on the first line paragraph [0015], the present application states "[v]erification data 94 comprises information associated with a query/response mechanism to enable the user of client 12 to independently recover a security credential 10 independent of a computer resource external to client 12" (emphasis added). As illustrated in this passage, the term "recover" is not limited to merely resetting a security credential. The term "recover," as used in the present application, is instead used to indicate an action that is utilized when the security credential is lost and/or is otherwise unavailable to a user. (Brief, pg. 8-17)

Examiner respectfully responds:

The examiner respectfully notes that the appellant's argument appears to be misleading. Namely, the passage of paragraph 15, as emphasized by the appellant, clearly does not provide a meaning for the term "recover". Furthermore, appellant's remarks appear to indicate that the appellant is uninterested in showing the meaning to the term "recover". Instead, the appellant vaguely suggests that the term "recover" should be interpreted as some sort of utilized "action".

The appellant's remarks fail to address the relevant section of the appellant's specification (as pointed to by the examiner when making the rejection), wherein the appellant explicitly gives an exemplary meaning to the term "recover":

> For example, as used herein, "recovering" security credential 100 includes enabling the user to independently retrieve security credential 100, enabling the user to independently reset security credential 100, and/or automatically having security credential 100 reset for the user by security module 70 without assistance from support personnel or an external computer resource. (par. 15, emphasis added)

The examiner respectfully notes that the appellant discloses, in plain language, that the term "recovering" may be interpreted as being limited to at least enabling the user to independently reset security credential.

Thus, the examiner does not believe paragraph 15 of the applicant's specification to have been improperly analyzed.

Appellant argues or asserts essentially that:

Conversely, Thompson discloses receiving a password from a user (FIG. 4, block 404), determining whether the received password is valid (FIG. 4, block 408), and changing the password (FIG. 4, blocks 412, 414, 420). As illustrated in FIG. 4, the password of Thompson is known, and the user is merely changing the known password to a new known password. Consequently, nothing in Thompson is "recovered" and thus, the Final Office Action has failed to establish a proper 35 U.S.C. §102(b) rejection. For at least these reasons, Appellants respectfully traverse this rejection, and submits that claim 14 is allowable in view of the cited art. (Brief, pg. 8-17)

Examiner respectfully responds:

As was noted above, the examiner again respectfully points out that the appellant discloses that the term “recovering" may be interpreted as being limited to at least enabling the user to independently reset security credential. Because Thompson, anticipates enabling the user to independently reset his password (i.e. “security credential”), the examiner maintains that Thompson anticipates “*enabling the user to recover the security credentia*l”.

Furthermore, while the examiner finds the appellant's allegation (i.e. resetting a password [i.e. "security credential"] may not be interpreted as "recovering a security credential”] to be incorrect based upon the evidence of record, the examiner respectfully notes that Thompson does not limit his disclosure to only resetting a security credential.

As noted within the above rejection, Thompson discloses that, via the query/response mechanism, the security module receives a "response from the user" (i.e. password), compares the received password with the stored password belonging to the user (fig. 6:606), and then based upon a valid "response", allows the password to be reset and stored such that the user is enabled to retrieve it at any time in case he/she should forget it (fig. 6:606, 610; 616; col. 9: lines 18-21). Thus, Thompson discloses that the user is enabled to *retrieve* his password, which consistent with the applicant's specification, may also be interpreted as a form of "recovering".

Clearly, the examiner respectfully points out, Thompson discloses both resetting and retrieving a security credential, each of which is explicitly disclosed by the applicant to be, at least, one form of "recovering" of a security credential. Thus, the examiner finds the appellant's arguments to be unpersuasive and maintains that Thompson discloses the claimed invention.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Jeffery Williams/

Examiner, Art Unit 2437

Conferees:

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437